## Claims

1. A method for managing user access information for access to one or more database network nodes, the method comprising:

storing database user authorization in a central directory, the database user authorization comprising a user role;

storing database user authentication information;

locally defining the user role at a network node;

receiving an access request from a user for the network node;

authenticating the user based upon the database user authentication information; and

granting the user privileges on the network node based upon the user role.

2. The method of claim 1 in which the central directory comprises a LDAP-compatible directory.

3. The method of claim 1 in which the database user authentication information is stored at the central directory.

4. The method of claim 1 in which the database user authorization is stored in a schema having a hierarchy of schema objects.

5. The method of claim 4 in which the hierarchy of schema objects comprises an enterprise role, wherein the enterprise role is associated with one or more users and one or more locally defined roles.

6. The method of claim 5 in which the privileges associated with the one or more locally defined roles are assigned to the one or more users.

7. The method of claim 4 in which the hierarchy of schema objects comprises a enterprise domain, wherein the enterprise domain comprises one or more enterprise roles.

8. The method of claim 7 in which each of the one or more enterprise roles is associated with one or more users and one or more locally defined roles.

9. The method of claim 7 in which the enterprise domain is associated with one or more network nodes.

10. The method of claim 1 in which the database user authorization is stored as one or more data objects in the central directory.

11. The method of claim 10 in which the one or more objects are stored in a security subtree in the central directory.

12. The method of claim 1 in which administrative access is controlled to one or more data objects in the central directory.

13. The method of claim 12 in which access control is implemented using an access control point associated with the one or more data objects in the central directory.

14. The method of claim 13 in which the access control point is associated with access policies for a subtree of the one or more database objects in the central directory.

15. The method of claim 13 in which the access control point is associated with access policies for a single entry for the one or more database objects in the central directory.

16. The method of claim 13 in which the access control point is associated with individually named users.

17. The method of claim 13 in which the access control point is associated with a group of users.

18. The method of claim 17 in which members of the group are associated with a set of access privileges associated with the access control point.

19. A system for managing user access information for one or more database network nodes, comprising:

a LDAP directory;

one or more database network nodes for which user access is sought; and

user access information data objects stored in the LDAP directory, the user access information data objects comprising authentication and authorization information.

20. The system of claim 19 in which the user access information data objects comprise a domain object that is associated with the one or more database network nodes.

21. The system of claim 20 in which the domain object is associated with an enterprise role.

22. The system of claim 21 in which the enterprise role is associated with a local database role.

23. The system of claim 22 in which the scope of the local database role is locally defined at a local database network node.

24. The system of claim 21 in which the enterprise role is associated with one more users.

25. The system of claim 24 in which each of the one or more users is associated with privileges defined for the enterprise role.

26. The system of claim 19 in which the user access information data objects comprise an access control point attribute.

27. The system of claim 26 in which the access control point attribute is established only if access control policies are established for a corresponding object.

28. The system of claim 26 in which the access control point attribute is associated with access policies for a subtree in the user access information data objects stored in the LDAP directory.

29. The system of claim 26 in which the access control point attribute is associated with access policies for a single entry in the user access information data objects stored in the LDAP directory.

30. The system of claim 26 in which the access control point attribute is associated with individually named users.

31. The system of claim 26 in which the access control point attribute is associated with a group of users.

32. The system of claim 31 in which members of the group are associated with a set of access privileges associated with the access control

33. The system of claim 19 in which the user access information data objects comprise a mapping object that maps an database user to a database schema.

34. The system of claim 33 in which the mapping object affects a single user.

35. The system of claim 34 in which the mapping object is associated with a full distinguished name.

36. The system of claim 33 in which the mapping object is associated with a plurality of users.

37. The system of claim 36 in which the mapping object is associated with a partial distinguished name.

38. The system of claim 21 in which the enterprise role is associated with local database roles from a plurality of database nodes.

39. A computer program product that includes a medium usable by a processor, the medium having stored thereon a sequence of instructions which, when executed by said

processor, causes said processor to execute a process for managing user access information for database network nodes, the process comprising:

storing database user authorization in a central directory, the database user authorization comprising a user role;

storing database user authentication information;

locally defining the user role at a network node;

receiving an access request from a user for the network node;

authenticating the user based upon the database user authentication information; and

granting the user privileges on the network node based upon the user role.